CONTINUATION OF APPLICATION FOR A SEARCH WARRANT

1. I, Kurt B. Schichtel, am a Special Agent of the Federal Bureau of Investigation (FBI). I have been so employed since August of 1992. I am currently assigned to the Kalamazoo Resident Agency in Kalamazoo County, Michigan. In my employment as an FBI Special Agent, I have investigated various types of federal criminal violations, including computer crimes, sexual exploitation of children, and child pornography matters. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

INTRODUCTION AND PURPOSE OF THE WARRANT

2. I make this continuation in support of an application for a search warrant to search computers and a digital storage compact disk (CD) belonging to DAVID JOSEPH HARWOOD for evidence, contraband, fruits, and instrumentalities of crime in violation of 18 U.S.C. §§ 2252A(a)(2) (distribution or receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography). The property or premises to be searched is identified in Attachment A, as follows:

a. **HP Pavilion desktop computer, Model 550-a114, Serial Number 4CI5430D04,**
b. **Acer Aspire desktop computer, Model T-180, Serial Number PTS560X07872909EC42714,**
c. **Compaq Presario 5000 desktop computer, Model 5UVME2, Serial Number 9129CGWZK516, and**
d. **An unmarked CD (Green).**

3. These items are currently in the custody of the Federal Bureau of Investigation, Kalamazoo Resident Agency. The items to be searched for and seized are described in Attachment B.

4. Pursuant to the provisions of 18 U.S.C. § 2256, "child pornography" means a visual depiction, the production of which involves the use of a minor engaging in sexually explicit conduct, including but not limited to various simulated or actual sex acts, or the lascivious exhibition of the genitals or pubic area.

5. I am familiar with the information contained in this continuation based on the investigation I have conducted, and based on information provided to me by other law enforcement officers/intelligence research specialists/computer examiners who have engaged in investigations involving the distribution of child pornography.

6. The facts in this continuation come from statements provided by DAVID JOSEPH HARWOOD during an interview, my personal observations during that interview, my training and experience, and information obtained from other agents and witnesses. Since this continuation is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities in violation of 18 U.S.C. § 2252A are presently located on the items identified in paragraph 2.

FACTUAL BACKGROUND OF INVESTIGATION

7. On November 14, 2015, at 10:36 Universal Time Code (UTC), automated systems at AOL, an Internet services company, identified the transmission of two emails with attachments suspected of containing child pornography. The emails were being sent from and to a single

account, kg8dr@aol.com. The emails were sent from an Internet-capable device assigned the Internet Protocol (IP) address 66.87.91.117. An IP address is a unique set of numbers assigned either for a unique session or an extended period of time to the device or place from which the Internet is being accessed. Both emails were captured and reviewed by AOL confirming they contained child pornography. On November 16, 2015, AOL referred the information including the emails, attachments, and transmission information to the National Center for Missing and Exploited Children (NCMEC). AOL also reported closing the account that same day (November 16, 2015) as a result of the confirmed presence of child pornography in the email attachments. AOL did not further examine the account, but its contents were preserved for possible further law enforcement investigation.

8. A review of the emails referred to NCMEC showed they were sent seven minutes apart at 5:28 AM and 5:35 AM local time. Neither email had any narrative or text, but an automated message on both indicated the emails were "Sent from my Virgin Mobile phone." Both emails contained the same file attachments. The attachments comprised 23 image files. Of those, 21 files contained depictions of nude females or females engaged in sexually explicit conduct. Eighteen (18) of the images appeared to be child pornography depicting a prepubescent child engaged in a sexual act with another person, either a child or an adult, and/or with a lascivious display of the genitals.

9. Among the 18 images of child pornography are the following examples:

a. Filename: 1016589_79.jpg is an image file that depicts a prepubescent female lying on her back naked, except for fishnet stockings. The child's legs are spread displaying her naked genital area. The child appears to be holding an object inserted into her vagina.

b. Filename: pbj_110_76.jpg is an image file that depicts a prepubescent female lying naked on a bed. The child's hands are covering her face, and her legs are bent at the knee and spread to display her naked genital area.

c. Filename: LC-645610_79.jpg is an image file that depicts a prepubescent female sitting on the floor. The child is visible from the waist up and is naked except for a paper eye mask. The child is engaged in an oral sex act on an adult male.

10. Copies of the images described in the paragraph above are available for judicial review. If the Court requests to view these images during its review of this application, the images will be filed as Attachment C to this application, and the United States Attorney's Office will request that the attachment remain sealed until further order of the Court. If the Court does not request to view the images, they will be retained by the United States Attorney's Office or the investigating agency for safekeeping without being filed as an attachment to this application.

11. FBI analysts working at NCMEC initiated further inquiries regarding this online activity in an attempt to identify and locate the person involved. Inquiry was made with AOL to identify the subscriber and the subscriber's location. Pursuant to a child exploitation administrative subpoena, AOL reported the email account kg8dr@aol.com was subscribed to DAVID HARWOOD, who reported his address at the time of establishing the account as 200 Snapdragon Street, Climax, Michigan 49034. AOL also provided records of online sessions for the account associated with kg8dr@aol.com. These records showed sessions accessing the account from August 2015 through November 2015 from various Internet service providers including Sprint and CTS Telecom. IP address 66.87.91.117, the IP address from which the child pornographic emails were sent, was determined to be an IP address belonging to Sprint, which

provides network services for Virgin Mobile telephone services. Of note, the AOL records showed that the kg8dr@aol.com account was concurrently accessing AOL services from a second IP Address, 67.219.200.168, at the same time the emails were transmitted. This IP Address belonged to CTS Telecom, a local telephone and Internet service provider in Western Michigan and servicing the communities of Climax, Battle Creek, Portage, Kalamazoo, and Scotts, Michigan.

12. This area of services includes the area where the Climax, Michigan, address is located that is associated with the kg8dr@aol.com account, as described in paragraph 11. Climax, Michigan is a village located in Kalamazoo County, within the Western District of Michigan.

13. The matter was referred to me for further investigation. I conducted records checks and investigated locally to determine if DAVID HARWOOD was residing in Climax, Michigan. I obtained records of the Michigan Department of Secretary of State for DAVID JOSEPH HARWOOD showing his current residence as 211 West Maple Street, Apartment 4, Climax, Michigan 49034. In addition, HARWOOD currently had a vehicle registered in his name bearing Michigan license plate 1LLA7. The address associated with this vehicle registration was also 211 West Maple Street, Apartment 4, Climax, Michigan 49034. On several occasions, I observed HARWOOD's vehicle parked outside the apartment building located at 211 Maple Street, Climax, Michigan.

14. The emails containing the child pornography on the kg8dr@aol.com account were sent from a cell phone on the Virgin Mobile network using the mobile IP address of 66.87.91.117, which made the exact location of the user at the time of sending difficult to ascertain. At the same time the user of the kg8dr@aol.com account was sending the emails, the

same account was also being accessed from the second IP address (67.219.200.168), serviced by CTS Telecom ISP. Pursuant to a subpoena, I obtained CTS Telecom records for the second IP address (67.219.200.168), which indicated that this second IP address was assigned to a person other than HARWOOD at a physical address other than HARWOOD's. Based on available background information and periodic spot checks, I could not determine any connection between HARWOOD and the individual to whom the CTS Telecom IP Address was assigned or to that individual's residence. Therefore, I could not definitively determine based on the available information at the time that HARWOOD was the person who sent the pornographic emails.

15. In an effort to determine if there was any further evidence relating to child pornography trafficking relating to HARWOOD on the kg8dr@aol.com account, I obtained a search warrant from this Court under docket number 1:16-MJ-00133 for the content of the email account. While there was saved content on the email account dating back to 2014, none of the available content or identifiable web activity related to child pornography trafficking.

16. A decision was made to conduct a "knock and talk" interview at HARWOOD's residence to determine if further information and evidence could be developed. On October 20, 2016, I contacted HARWOOD at his current residence, 211 West Maple Street, Apartment 4, Climax, Michigan 49034, to conduct a "knock and talk" interview. I was accompanied by Special Agent Mark A. Waldvogel. After identifying ourselves and advising HARWOOD that we wanted to speak to him regarding an investigation relating to online activity, HARWOOD voluntarily admitted us into his apartment. Before continuing the interview, I immediately told HARWOOD that the online activity involved emails with child pornography attachments on an AOL email account, kg8dr@aol.com, which was reported to belong to him. I told HARWOOD that he need not talk to us. I also informed HARWOOD he was not under arrest nor would he be

arrested since there were no charges of any type against him. I also told him at the outset that I did not have any search warrant for his residence or his computers. HARWOOD agreed to talk to us.

17. HARWOOD almost immediately said he thought he knew about the email incident. He was then simply asked if he had child pornography in his possession now. HARWOOD said he "probably" had child pornography on his computer. He then pointed to a computer on the floor next to a computer table in the living room where the interview was being conducted. There were actually two desktop computers, one atop of the other, sitting in plain view of the interviewing agents.

18. I asked HARWOOD if he would consent to a search of the two computers that he had identified. I advised him the search would be for child pornography. I advised him again that I did not have a search warrant and that he would have to consent to any search. I also told him I had a preview software program with which I could conduct a preliminary search onsite. HARWOOD said we could look at the computer using the preview software.

19. Before doing so, I completed an FBI Consent to Search form identifying the two computers sitting on the floor. The computers were identified as an HP Pavilion desktop computer, Model 550-a114, and an Acer Aspire desktop computer, Model T-180, with the descriptive information written on the Consent to Search form. Portions of the FBI Consent to Search form state the following:

a. I have been advised of my right to refuse consent.

b. I give this permission voluntarily.

c. I authorize these agents to take any items which they determine may be related to their investigation.

20. I read the Consent to Search form to HARWOOD. With reference to the portion of the consent authorizing the agents to take any items related to the investigation, I told HARWOOD that I would have to take the computers if I saw child pornography on them. I asked him if he was willing to consent to the search. He said he would. I asked him to further signify his consent by signing the consent form, which he did.

21. I then initiated the onsite search of the HP Pavilion desktop computer using a preview software routinely used by FBI personnel in "knock and talk" situations. I have received training in the use of preview software. In conducting the searches on the HP Pavilion desktop computer, the software subsequently identified over six thousand image files of various types. In reviewing these image files, I saw a several hundred images that I believed would constitute child pornography. A number of these images were saved on the computer in a folder named "mine." I saved three images from a single series that appeared to constitute child pornography as examples of the content I observed in the preview. There were a large number of similarly named series with similar content. The files saved are identified as follows:

a. Filename: etaphro17092001an12.jpg depicts a prepubescent female, likely under the age of 10, posing fully nude in front of a brick wall with her arms stretched out holding a mesh garment. The image depicts her naked genital area in a lascivious manner.

b. Filename: etaphro17092001an14.jpg depicts the same prepubescent female in the same general scene but with closer perspective, posing fully nude in front of a brick wall with her arms stretched out holding a mesh garment. The image again depicts her naked genital area.

c. Filename: etaphro17092001an02.jpg depicts the same prepubescent female,

posing fully nude with her arms stretched out holding a mesh garment. The image depicts her naked genital area. This image appears to be in an abandoned industrial building.

22. Copies of the images described in the paragraph above are available for judicial review. If the Court requests to view these images during its review of this application, the images will be filed in Attachment C to this application, and the United States Attorney's Office will request that the attachment remain sealed until further order of the Court. If the Court does not request to view the images, they will be retained by the United States Attorney's Office or the investigating agency for safekeeping without being filed as an attachment to this application.

23. HARWOOD continued talking to the interviewing agents and answering questions in a candid manner. HARWOOD said he had been collecting child pornography for up to 15 years and thought he might have "thousands" of images on the computers. He obtained child pornography images from online newsgroups. HARWOOD confirmed the kg8dr@aol.com email was his own. When shown the images attached to the email detected by AOL, HARWOOD said he recalled them. HARWOOD could not explain the logons to his account from the IP address for CTS telecom, but he reported using a Virgin Mobile hotspot on his computer to access the Internet and, at times, using unsecured wireless access points which he presumed were in his own apartment building.

24. While conducting the preview search of the HP Pavilion desktop, HARWOOD said the Acer Aspire desktop computer, for which he had also consented to a search, was no longer used by him because it did not boot up properly. He stated though that the Acer Aspire also had child pornography saved on it. When asked if there was any other computer which he knew contained child pornography, HARWOOD voluntarily identified an older computer sitting

on the floor on the other side of the computer table. This computer was a Compaq Presario 5000 desktop computer that no longer worked and did not have a power supply. The Compaq Presario 5000 still had an installed hard drive. When asked if he had any digital media, such as thumb drives, SD cards, or disks that he knew to contain child pornography, HARWOOD stood up, walked to the computer table, and picked up a green compact disk (CD) that was otherwise unmarked. He handed me the CD. HARWOOD said that was the only other media item that had child pornography on it. HARWOOD said the computers likely had much of the same materials since he had transferred files from one computer to the next whenever he purchased a new computer.

25. Inasmuch as I had already viewed images I believed to be child pornography on HARWOOD's HP Pavilion computer and HARWOOD had admitted to collecting child pornography from the Internet for some period of years and storing the child pornography on the other computers and on the CD he handed to me, I believed these items to contain evidence of possession of child pornography and possible receipt of child pornography. I also knew or believed these items contained contraband material in the form of child pornography images. As such, I secured the items and seized them. I informed HARWOOD I would seek a search warrant to conduct any further search of the items, which is the purpose of this continuation. HARWOOD said he understood the reason the items were being seized. I provided HARWOOD with a receipt for the items, which he signed. SA Waldvogel and I removed the HP Pavilion desktop, the Acer Aspire desktop, the Compaq Presario 5000 desktop, and the green unmarked CD from the premises. No other property was removed from HARWOOD's residence.

26. I later processed the items seized as evidence in this investigation. The items seized are those detailed in Attachment A and described below:

a. HP Pavilion desktop computer, Model 550-a114, Serial Number 4CI5430D04,

b. Acer Aspire desktop computer, Model T-180, Serial Number PTS560X07872909EC42714,

c. Compaq Presario 5000 desktop computer, Model 5UVME2, Serial Number 9129CGWZK516, and

d. An unmarked CD (Green).

27. While HARWOOD's signed consent to search included both the HP Pavilion and the Acer Aspire, I did not conduct an onsite search on the Acer Aspire because of HARWOOD's statements regarding its service condition and because it was not already connected to peripheral hardware such as a monitor and keyboard, which would have been required to conduct the search. Because of the absence of a power supply in the Compaq Presario, an onsite search was also not possible, nor had HARWOOD identified the computer to us at the time we were preparing the Consent to Search. Similarly, HARWOOD only identified the CD as having child pornography after his possession was already confirmed through the consent search of the HP Pavilion. Therefore, I seized the Compaq Presario and the CD on probable cause that they contained contraband, based on HARWOOD's admissions that they contained child pornography. I seized the HP Pavilion and Acer Aspire computers based on HARWOOD's consent.

28. The preview search I conducted on the HP Pavilion pursuant to the consent was a limited field search. It did not search for or identify all of the evidence contained on the hard drive(s). As an example, the preview search cannot identify previously deleted files of any type. As a result, there may be evidence regarding the source of child pornography and methods and

means of collection. Only a full forensic examination of the property can identify all of the evidence, contraband, fruits, and instrumentalities of crime in violation of 18 U.S.C. §§ 2252A(a)(2) (distribution or receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography), as described further in Attachment B. As such, the Court's authorization is being sought to search the contents of the computers and CD based on the probable cause set forth herein that HARWOOD possessed child pornography on the HP Pavilion and stated that the other property identified in Attachment A has child pornography currently saved to them and would therefore have been used in the receipt and possession of child pornography.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

29. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography. There is probable cause to believe that HARWOOD is a collector of child pornography based on the length of time and number of devices HARWOOD stated he used to seek out child pornography. Characteristics common to people involved in the receipt and possession of child pornography include that they:

a. Generally have a sexual interest in children and receive sexual gratification viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including in hard copy and/or digital formats.

c. Generally maintain their collections in a safe, secure, and private environment, most often where they live and/or on their person. These images

and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, Internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media).

d. Generally maintain their collections for a long period of time, due to the illegal nature of the material and their high level of interest in it;

e. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Such correspondence may take place, for example, through online bulletin boards and forums, Internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person.

30. There is probable cause to believe that HARWOOD is a child pornography collector and that the seized devices, identified in Attachment A, contain evidence of child pornography activity.

SPECIFICS OF SEARCHING COMPUTER SYSTEMS

31. Computers and Internet-capable devices facilitate the collection, receipt, and distribution of child pornography. The Internet and the nature of personal computers afford collectors of child pornography several different venues for obtaining, viewing, and trading child

pornography in a relatively secure and anonymous fashion.

32. Storage capacity of computers and portable storage media, such as CDs, has grown tremendously within the last several years. They can store thousands of images at very high resolution, are easily transportable, and are relatively inexpensive.

33. As with most digital technology, communications made from a computer device are often saved or stored on that device. Storing this information can be intentional, for example, by saving an email as a file on the computer or saving the location as a "favorite" website in a "bookmarked" file. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be stored automatically in many places, such as temporary files or Internet Service Provider (ISP) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

34. A forensic examiner often can recover evidence that shows whether a computer device contains peer-to-peer software, when the device was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that date remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of

time before they are overwritten.

35. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

36. Searches and seizures of evidence from computers and computer devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to

specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

37. Forensic examiners can also find the presence or absence of certain software and programs to determine who controlled a computer at a given time. Such evidence includes: viruses, Trojan horses, spyware, malware, and other forms of malicious software; the presence or absence of security software designed to detect malicious software; the lack of malicious software; and the presence or absence of software designed to protect a device from infiltration, access, or control by another person or entity, which may include pop-up blockers, security software, password protection, and encryption. Forensic examiners can also find evidence of software or programs designed to hide or destroy evidence.

38. The time period required for a complete, safe, and secure forensic examination of the computer and storage media is uncertain. The Government will make available for pick-up within a reasonable time all items found not to contain any contraband or material to be seized pursuant to the warrant and all hardware and software no longer needed for examination purposes. In conducting the search, the forensic examiner and agents will examine files regardless of their name because such names and file extensions can be altered to conceal their actual content. Because of the volume of data to be searched and the need to complete the

examination in a reasonable time, the forensic examiner will also use computer techniques such as keyword searches that may result in the display of irrelevant materials.

39. Retention of any computers would be warranted, if any child pornography is found thereon, in order to permit forfeiture of those computers and related properties as instrumentalities of the crime, pursuant to 18 U.S.C. §§ 2253(a)(3) and 2254(a)(2).

CONCLUSION

40. Based on the above factual information set forth above, I respectfully submit that there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of crime in violation of 18 U.S.C. §§ 2252A(a)(2) (distribution or receipt of child pornography) and 2252A(a)(5)(B) (possession of child pornography) exists on the seized property belonging to DAVID JOSEPH HARWOOD, described in Attachment A.

41. I therefore respectfully request that the attached warrant be issued authorizing the search of the property listed in Attachment A, currently in the custody of the FBI in Kalamazoo, Michigan, and seizure of the items listed in Attachment B.